



Exhibit 4

Charted claim:
Method claim:1

US8917843B2	SecureLogix - Call Secure™ managed service (“The accused instrumentality”)
<p>1. A method performed by a call control unit for controlling incoming and outgoing calls at a user's premise, the method comprising:</p> <p>receiving an indication of an incoming call at a call control unit communicatively coupled to or resident within a telephone, the call control unit being located at the user's premise and positioned between a telecommunication service provider providing the incoming call and the telephone, the indication including identification information for the incoming call;</p>	<p>The accused instrumentality discloses a method (e.g., call security protection method) performed by a call control unit (e.g., Robocall/spam call protection unit of the Call Secure™) for controlling incoming and outgoing calls (e.g., controlling calls through Call Secure™) at a user's premise (e.g., user smartphone installed with Call Secure™), the method comprising receiving an indication of an incoming call (e.g., receiving an incoming call from the caller directed to smartphone with Call Secure™ installed) at a call control unit (e.g., Robocall/spam call protection unit of the Call Secure™) communicatively coupled to or resident within a telephone (e.g., present within the smartphone using Call Secure™ managed service), the call control unit (e.g., Robocall/spam call protection unit of the Call Secure™) being located at the user's premise (e.g., user smartphone installed with Call Secure™) and positioned between a telecommunication service provider (e.g., calling service provider) providing the incoming call (e.g., incoming call initiated by the caller) and the telephone (e.g., called user smartphone), the indication (e.g., incoming call indication) including identification information for the incoming call (e.g., the incoming call includes caller name, ID, phone number, etc.).</p> <p>As shown, Call secure app includes call control feature for preventing calls from robocallers, spammers, etc. When a caller dials the number to a called user phone, the incoming call is received at the Robocall/spam call blocking unit of the Call secure app installed within the caller user smartphone. The accused instrumentality identifies robocallers, spammers, etc., using the caller information such as caller name, phone number, etc.</p>

	<div> What We Do Research & Tech About Resources Partners</div> <div><h1>CALL SECURETM</h1><p>managed service</p></div> <div><p>Reduce costs and secure your business lines and contact centers from attack, disruption, fraud & abuse.</p></div> <div>Download Brochure</div> <div> Watch 30-sec intro video</div> <div>https://securelogix.com/voice-network-security/</div>
--	---

CALL SECURITY +

The Call Secure™ managed service delivers superhero-level call security protection.

The Call Secure™ managed service combines the power of cutting-edge technology with the most experienced call security service team in the business. Our proprietary technology sits at the edge of your TDM or SIP voice network and sorts good traffic from bad to reduce unwanted calls and keep your voice network safe and secure from attack. This technology is delivered and managed by our industry-leading team of call security experts who work every day to ensure you and your business always come out on top.

<https://securelogix.com/voice-network-security/>

Benefits

- Protect against voice network attacks (SIP Security)
- Proactive monitoring of new attacks and malicious calls
- Call fraud, spoofing and robocall protection
- Reduce call spam and unwanted nuisance calls
- Supported by our best-in-class service team




SecureLogix offers voice security technology

<https://securelogix.com/voice-network-security/>



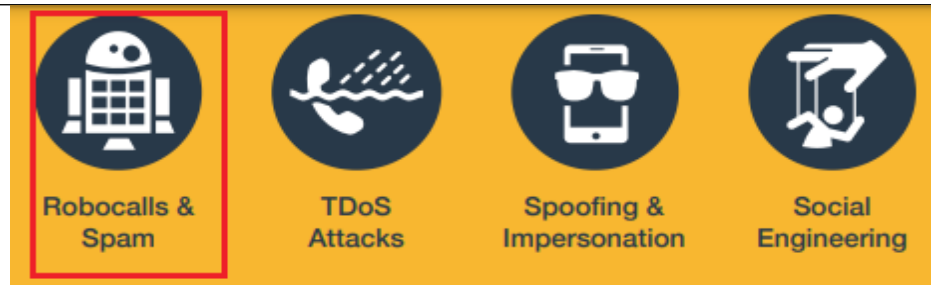
<https://securelogix.com/voice-network-security/>



	 <p>Caller Profiles</p> <p>Red List is continuously updated with caller profile information helping us to identify and block nuisance callers.</p> <p>https://securelogix.com/voice-network-security/</p>
<p>querying, by the call control unit, a server external to a telecommunication service provider providing the call and the telephone to determine whether additional information regarding a caller associated with the identification information</p>	<p>The accused instrumentality discloses querying, by the call control unit e.g., Robocall/spam call protection unit of the Call Secure™), a server (e.g., server of the accused instrumentality) external to a telecommunication service provider (e.g., calling service provider) providing the call and the telephone (e.g., incoming call on the called user smartphone) to determine whether additional information (e.g., additional information such as red list database, etc.) regarding a caller associated with the identification information (e.g., caller identification information includes caller name, ID, phone number, etc.) is stored within a database (e.g., e.g., determine whether caller number is stored in red list database) communicatively coupled to the server (e.g., server of the accused instrumentality), the database (e.g., red list database) storing additional information associated with unwanted callers (e.g., storing unwanted harassing callers), the additional information (e.g., additional information such as red</p>

<p>is stored within a database communicatively coupled to the server, the database storing additional information associated with unwanted callers, the additional information including a user-configurable list of at least one of desired and undesired callers and being associated with a preferred operation to be performed on a call associated with the additional information, and if so, performing a first operation on the incoming call responsively to the additional information, the first operation corresponding to the preferred operation associated with the additional information, otherwise, performing a second operation on the incoming call responsively to an</p>	<p>list database, etc.) including a user-configurable list (e.g., call secure team configured list) of at least one of desired and undesired callers (e.g., harassing callers, spam callers, robocallers, etc.) and being associated with a preferred operation (e.g., preferred operation for spam callers - blocking the spam call or forwarding the verified call) to be performed on a call associated with the additional information (e.g., additional information such as red list database, etc.), and if so, performing a first operation (e.g., blocking the call) on the incoming call responsively to the additional information (e.g., when the caller number is stored in red list database), the first operation (e.g., blocking the call) corresponding to the preferred operation (e.g., incoming calls that are already present in red list are directly blocked and not forwarded to the called user) associated with the additional information (e.g., additional information such as red list database, etc.), otherwise, performing a second operation on the incoming call responsively to an absence of the additional information (e.g., forwarding the call using call screening process when caller number is absent in red list database).</p> <p>As shown, when the caller dials the number, the Robocall/spam call protection unit of the Call Secure™ queries the app server to determine whether the caller phone number is present in red list database, where the red list database is preconfigured caller profile database stored at server including harassing callers profiles to identify and block spam/robocalls. If the server determines that the caller number is present in the red list database, the call control unit performs preferred operation such as blocking the call (first operation). If the server determines that the caller number is absent in the red list database, the Robocall/spam call protection unit routes the call to the called user based on call screening process (a second operation) including solving puzzles, etc.</p>
---	--

absence of the
additional information;



SUPERHERO-LEVEL SERVICE

The best technology in the world is only as good as the people behind it.

The SecureLogix® Call Secure™ Managed Service is powered by a team of call security experts with more than 400 years of collective experience. No team secures more enterprise voice networks, phone lines and calls than SecureLogix.

The Call Secure team also builds and maintains the Red List™ call threat database — a proprietary dataset of national harassing callers, voice spammers and call attack signatures.

Red List is powered by the intelligence we gather from the enterprise voice attacks and malicious caller interactions that we see everyday. Every Call Secure customer benefits from Red List and it is a key ingredient in how we are able to continuously improve our ability to protect calls and network resources in a landscape where the threats are constantly changing and evolving.

<https://go.securelogix.com/downloads/flyers/call-secure>

RED LIST™

caller profile database

The Red List™ caller profile database is our proprietary database of harassing callers and attack signatures. A standard component of the Call Secure™ managed service solution, the Red List database is founded on 20 years of voice network protection experience.

Red List leverages our broad and deep view of enterprise voice attacks and malicious caller interactions and we use this data to keep your voice network safe and secure day in and day out.



Caller Profiles

Red List is continuously updated with caller profile information helping us to identify and block nuisance callers.



Attack Signatures

We catalog known and emerging attack signatures so attacks can be quickly identified and defeated.

<https://securelogix.com/voice-network-security/>

Governments and industry continue to work toward broad implementation of STIR/SHAKEN and its call attestation benefits. STIR/SHAKEN can indeed provide a substantial and credible means to help verify call identity. Even still, broad acceptance of STIR/SHAKEN alone will not solve all of the issues surrounding call identification, security and trust for the enterprise. Many gaps will remain, and enterprise and contact center environments will remain vulnerable to many types of robocalls and spoofed calling attacks.

A broader architecture and set of technologies for call security and trust is required, along with an intelligent and efficient means to unify and optimize all of it. If properly orchestrated, this broader framework can powerfully lever STIR/SHAKEN across an ecosystem of other industry metadata sets, technology plugins, and industry fraud tools to deliver the most useful call identification results at the lowest cost. This approach extends STIR/SHAKEN to help complete the call verification and security puzzle in a highly affordable and scalable way for the enterprise.

<https://securelogix.com/events/stir-shaken-and-call-verification/>

STIR/SHAKEN Implementation



The implementation of the FCC's STIR/SHAKEN protocol is a legal response to consumers' clamors. It aims to eliminate call spoofing by using call authentication technology. Currently, the technology also alerts consumers if they call they receive is valid.


<https://calleridreputation.com/blog/understanding-how-shaken-tokens-work/>

Authenticator

The STI-AS and STI-VS expose the REST API to the Authenticator. This is the piece of the carrier network puzzle that uses authentication and signing services to make and verify digital signatures from the carriers. Moreover, in some protocols, the STI-AS and STI-VS have a fixed anchor position—with the

<https://calleridreputation.com/blog/understanding-how-shaken-tokens-work/>



	 <p>using advanced call filtering technology</p> <p>https://securelogix.com/voice-network-security/</p>
<p>receiving an indication at the call control unit that the incoming call is undesired; and</p>	<p>The accused instrumentality discloses receiving an indication (e.g., robocall or spam call indication) at the call control unit (e.g., Robocall/spam call protection unit of the Call Secure™) that the incoming call is undesired (e.g., incoming call is identified as a Robocall/spam call).</p> <p>As shown, Call Secure™ managed service delivers call security protection for voice network by identifying and filtering unwanted incoming calls received from the spam callers, robocallers, etc. The identified robocall or spam call indication is received at the Robocall/spam call protection unit of the Call Secure™.</p>

CALL SECURITY +

The Call Secure™ managed service delivers superhero-level call security protection.

The Call Secure™ managed service combines the power of cutting-edge technology with the most experienced call security service team in the business. Our proprietary technology sits at the edge of your TDM or SIP voice network and sorts good traffic from bad to reduce unwanted calls and keep your voice network safe and secure from attack. This technology is delivered and managed by our industry-leading team of call security experts who work every day to ensure you and your business always come out on top.

<https://securelogix.com/voice-network-security/>

Benefits

- Protect against voice network attacks (SIP Security)
- Proactive monitoring of new attacks and malicious calls
- Call fraud, spoofing and robocall protection
- Reduce call spam and unwanted nuisance calls
- Supported by our best-in-class service team

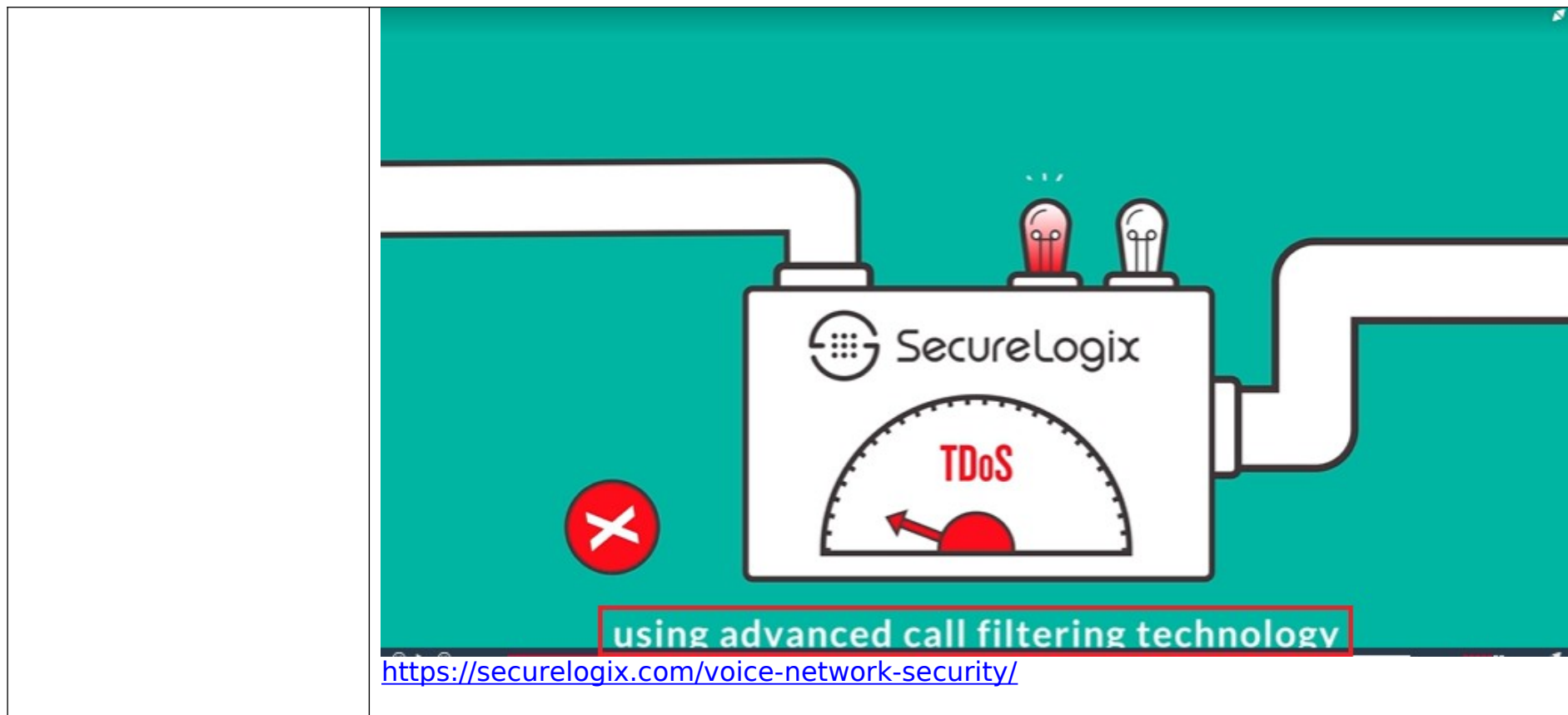


SecureLogix offers voice security technology

<https://securelogix.com/voice-network-security/>



<https://securelogix.com/voice-network-security/>



	<p>RED LIST™ <u>caller profile database</u></p> <p>The Red List™ caller profile database is our proprietary database of harassing callers and attack signatures. A standard component of the Call Secure™ managed service solution, the Red List database is founded on 20 years of voice network protection experience.</p> <p>Red List leverages our broad and deep view of enterprise voice attacks and malicious caller interactions and we use this data to keep your voice network safe and secure day in and day out.</p> <div data-bbox="1496 384 2058 911">  <p>Caller Profiles</p> <p>Red List is continuously updated with caller profile information helping us to identify and block nuisance callers.</p>  <p>Attack Signatures</p> <p>We catalog known and emerging attack signatures so attacks can be quickly identified and defeated.</p> </div> <p>https://securelogix.com/voice-network-security/</p>
<p>automatically adding the identification information for the undesired incoming call to the user-configurable list of undesired caller.</p>	<p>The accused instrumentality discloses automatically (e.g., automatically blocking) adding the identification information (e.g., caller identification such as caller number, name, etc.) for the undesired incoming call (e.g., incoming Robocall/spam call) to the user-configurable list of undesired caller (e.g., red list database is updated with newly identified spam call, robocall, etc.).</p> <p>As shown, Call Secure™ managed service delivers call security protection for voice network by identifying and filtering unwanted incoming calls received from the spam callers, robocallers, etc. based on red list database. The identified robocall or spam calls are automatically blocked and added to the red list database. The red list database is</p>

continuously updated with caller profile information such as caller number, name, etc. to identify and block spam callers.

CALL SECURITY +

The Call Secure™ managed service delivers superhero-level call security protection.

The Call Secure™ managed service combines the power of cutting-edge technology with the most experienced call security service team in the business. Our proprietary technology sits at the edge of your TDM or SIP voice network and sorts good traffic from bad to reduce unwanted calls and keep your voice network safe and secure from attack. This technology is delivered and managed by our industry-leading team of call security experts who work every day to ensure you and your business always come out on top.

<https://securelogix.com/voice-network-security/>

Benefits

- Protect against voice network attacks (SIP Security)
- Proactive monitoring of new attacks and malicious calls
- Call fraud, spoofing and robocall protection
- Reduce call spam and unwanted nuisance calls
- Supported by our best-in-class service team

RED LIST™

caller profile database

The Red List™ caller profile database is our proprietary database of harassing callers and attack signatures. A standard component of the Call Secure™ managed service solution, the Red List database is founded on 20 years of voice network protection experience.

Red List leverages our broad and deep view of enterprise voice attacks and malicious caller interactions and we use this data to keep your voice network safe and secure day in and day out.



Caller Profiles

Red List is continuously updated with caller profile information helping us to identify and block nuisance callers.



Attack Signatures

We catalog known and emerging attack signatures so attacks can be quickly identified and defeated.

<https://securelogix.com/voice-network-security/>



Robocalls &
Spam



TDoS
Attacks



Spoofing &
Impersonation



Social
Engineering

SUPERHERO-LEVEL SERVICE

The best technology in the world is only as good as the people behind it.

The SecureLogix® Call Secure™ Managed Service is powered by a team of call security experts with more than 400 years of collective experience. No team secures more enterprise voice networks, phone lines and calls than SecureLogix.

The Call Secure team also builds and maintains the Red List™ call threat database — a proprietary dataset of national harassing callers, voice spammers and call attack signatures.

Red List is powered by the intelligence we gather from the enterprise voice attacks and malicious caller interactions that we see everyday. Every Call Secure customer benefits from Red List and it is a key ingredient in how we are able to continuously improve our ability to protect calls and network resources in a landscape where the threats are constantly changing and evolving.

<https://go.securelogix.com/downloads/flyers/call-secure>



Caller Profiles

Red List is continuously
updated with caller
profile information
helping us to identify and
block nuisance callers.

<https://securelogix.com/voice-network-security/>



<https://securelogix.com/voice-network-security/>

